(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 719 045 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.06.1996 Bulletin 1996/26

(51) Int. Cl.[6]: **H04N 7/167**

(21) Application number: **95119605.4**

(22) Date of filing: **13.12.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **13.12.1994 JP 309292/94**

(71) Applicant: **MITSUBISHI CORPORATION**
Chiyoda-ku Tokyo 100 (JP)

(72) Inventor: **Saito, Makato**
Tama-shi, Tokyo (JP)

(74) Representative: **Neidl-Stippler, Cornelia, Dr.**
Rauchstrasse 2
D-81679 München (DE)

(54) Crypt key system for broadcast programmes

(57) The invention relates to a crypt key system applicable to a television system, a database system or an electronic commercial transaction system or the like. This system consists of a broadcasting station 11, a database 12, a receiving apparatus 14, a data communication apparatus 15 and a user terminal 18. As a crypt key system, a secret-key cryptosystem, a public-key cryptosystem, and a digital signature system are used. The keys used in the system are either encrypted or remain uncrypted to be supplied by broadcasting. The present invention is effective in the prevention of an unjustified use of the database system, managing copyrights, and in a pay-per-view system and a video-on-demand system. Further, the present invention is effective in realizing an electronic market which uses an electronic data information system.

EP 0 719 045 A2

Printed by Rank Xerox (UK) Business Services
2.12.4/3.4

Description

Background of the Invention

Field of the Invention

The present invention relates to a crypt key system that is used in a commercial trade or the like which uses a television system, a database system or an electronic data interchange.

Prior Art

In information oriented society of today, in addition to a normal terrestrial broadcasting, satellite broadcasting which is referred to as a broadcasting satellites (BS) and communication satellites (CS) or cable TV broadcasting which is referred to as CATV (cable television) using coaxial cables or optical cables is getting prevalent.

In a satellite broadcasting or CATV broadcasting which distributes several tens of channels at the same time, scrambled channels of such as films, sport events, and music which cannot be viewed through a comprehensive contracts are provided in addition to unscrambled general channels. In order to view these channels, it is necessary to subscribe to descramble the channels; however, normal subscription period is about one month unit, and it is impossible to view through temporary contracts.

The inventor of the present invention proposed in the Japanese Patent Application Laid-Open No. 6-46419 and the Japanese Patent Application Laid-Open No.6-141004 a system in which users obtain a viewing permit key from a charging center via a communication line and charged, and descrambles programs scrambled each by respectively different scramble pattern, using the viewing permit key to view the programs; proposed in the Japanese Patent Application Laid-Open No. 6-132916 an apparatus for the operation.

In these system and apparatus, those who wish to use scrambled programs request for viewing to the charging center via a communication line by using a communication apparatus. The charging center transmits the viewing permit key to the communication apparatus corresponding to the request for viewing while charging and collecting a fee.

Users, on receiving the viewing permit key with the communication apparatus, transmits the viewing permit key via direct means connecting the communication apparatus and the receiving apparatus or via indirect means such as flexible disks or the like. The receiving apparatus to which the viewing permit key is transmitted descrambles the programs with the viewing permit key and then, the users use the programs.

Japanese Patent Application Laid-Open No. 6-132916 describes a system and an apparatus for sell and rent of a tape or a disk on which a plurality of data scrambled with a different scramble pattern respectively are recorded to supply the viewing permit key with IC cards or the like and use a specific data.

In addition, in these days of information- oriented society, a database system has been propagated for mutually using data which are kept independently by each computer by constituting a computer communication network by LAN (local area network), WAN (wide area network), and Inter-Net system mutually connecting these networks.

In the meantime, a technology has been developed for reducing the information amount by compressing a television moving picture signal which could not be digitized because of a huge amount of information as a result of digitization, to enable practical digitalization. So far, H.261 standard for video conference, JPEG (joint photographic image coding experts group) standard for static pictures, MPEG 1 (moving picture image coding experts group 1) standard for storing pictures and MPEG 2 corresponding to the present telecast and the high definition telecast from the television broadcasting are prepared.

The digitization technology using these picture compression technology is used for the television broadcasting or the video picture recording. In addition, even television moving picture data which could not be dealt with before can be dealt with now. Then, the "multimedia system" which deals with various data dealt with by the computer and the digitized television moving picture data has been focused as a future technology.

This multimedia system is also incorporated in the data communication and can be used as one data on the database.

While the scope of usage of the database is expanded, the method for charging for the data usage on the database, and the method for dealing with copyright problems generated by copying, transmitting other than direct usage of data, and also the secondary exploitation right problem generated as a result of data edition have become important problems.

To safely deal with charging and copyrights process, it is required that the data cannot be used by users other than authorized users, and data encryption is the best means for it.

In addition, an electronic market system has been investigated for converting information in various kinds of transaction which has been carried out by paper documents so far, into an electronic data to execute electronic transaction by using the electronic data interchange for transmitting and receiving data by the data communication technology. In addition, an investigation is also made on the possibility of carrying out an electronical settlement on the electronic commercial transaction system.

In the commercial transactions, the reliability on the transaction details is required and the security in the settlement is required. Consequently, in the electronic commercial transaction system and electronic settlement system in which such reliability and security are

demanded, it is required that the data is encrypted so that the data will not be falsified or used unjustifiedly.

In these television system, database system or electronic commercial transaction system or the like, the data is encrypted and thus a crypt key is required for decrypting the encrypted data to us. And the crypt key must be given to data users; however, the processing is very troublesome because security and reliability are demanded.

In the structure of the present invention, data cryptology acts an important part. In the beginning, a general explanation will be made on the data cryptology.

In the data cryptology, the case in which the plaintext data M is encrypted by using a crypt key K to obtain a cryptogram data C is represented:

$$C=E(K, M),$$

and the case in which the cryptogram data C is decrypted by using the crypt key K to obtain the plaintext data M is represented:

$$M=D(K, C)$$

As a typical method for the data cryptography technology, there are a secret-key cryptosystem and a public-key cryptosystem. The secret-key cryptosystem is a cryptosystem in which same secret key Ks is commonly used in encryption and decryption

$$Cmks=E(Ks, M)$$

$$M=D(Ks, Cmks)$$

The public- key cryptosystem is a cryptosystem in which a key for encryption and a key for decryption are used as crypt keys, and the key for encryption is laid open but the key for decryption is not open. The key for encryption is referred to as a public-key Kb while the key for decryption is referred to as a private-key Kv. To use this cryptosystem, an information sender encrypts the plaintext data M by the pubic-key Kb of a receiver

$$Cmkb=E(Kb, M),$$

and the receiver receives the data and decrypts it by a private-key Kv to obtain the plaintext data M

$$M=D(Kv, Cmkb).$$

In this public-key cryptosystem, cryptanalysis is very dificult.

As an application of the data cryptography technology, digital signature is performed as an electronic data authentication means to ensure the reliability of the data.

The digital signature is used a secret key or a public-key. Generally, the public-key is used in the digital signature.

In the digital signature which is carried out by using the public-key, the signer obtains a digital signature by encrypting a document m to which the document M is compressed with hash algorithm, using the private-key Kv of the signer:

$$Smkv=E(Kv, m)$$

and transmits the original document M or the compressed document m and the digital signature Smkv to the receiver.

The receiver decrypts the digital signature Smkv by using the public-key Kb of the signer

$$m'=D(Kb, Smkv).$$

When m'=m is established, it is recognized that the signature is correct.

As a method for providing these crypt keys to users, the inventor of the present invention proposed an invention entitled "crypt key system" in the prior Japanese Patent Application No. 6-70643.

In the generally practiced crypt key system, the crypt key is provided only to users while the crypt key is provided to persons other than the users in the crypt key system of this prior invention.

Fig. 1 shows the structure of the crypt key system proposed in the Japanese Patent Application No. 6-70643.

This system comprises a broadcasting station 1 for multiplex boadcasting such as BS, CS, terrestrial broadcasting or FM or the like or data broadcasting, a database 2, a charging center 3, a receiving apparatus 4, data communication apparatus 5 and a user's terminal 8.

The broadcasting station 1 and the database 2, and the database 2 and the charging center 3 are connected to each other via a communication line such as a dedicated line or the like or flexible disc or the like. The database 2 and the data communication apparatus 5 are connected by a communication line 7 such as a communication line or CATV line.

The broadcasting station 1 and the receiving apparatus 4 are connected with the broadcasting radio wave 6. The receiving apparatus 4 and the user terminal apparatus 8, and the data communication apparatus 5 and the user terminal 8 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc.

In Fig. 1, what is shown with a solid line is a path of information which is not encrypted. What is shown with a broken line is a path of data which is encrypted.

In this system, the database 2 preliminarily supplies a permit key Kp (hereinafter referred to as a "permit key") including the crypt key Kd which is different from one data to another to the broadcasting station 1. The permit key Kp is explained in such a manner that the permit key Kp constitutes the crypt key Kd only for better understanding.

In some cases, the crypt key Kd is supplied without being encrypted, and in other cases, it is encrypted by using the common crypt key K0

$$Ckdk0=E(K0, Kd),$$

and is supplied as an encrypted crypt key Ckdk0.

In the case where the crypt key Kd is encrypted and supplied, a common crypt key K0 for decrypting the encrypted crypt key Ckdk0 is supplied to users. This common crypt key K0 is supplied when users register with the database, or it is supplied to the users together with the encrypted data Cmkd when the encrypted data Cmkd is transmitted.

(a) In the case where the crypt key is not encrypted:

In this crypt key system, the broadcasting station 1 broadcasts the crypt key Kd supplied from the database 2, by using the radio wave 6.

The receiving apparatus 4 supplies the received crypt key Kd to the user terminal 8 so that the user terminal 8 stores the received crypt key Kd in a recording medium such as a semiconductor memory, a flexible disc, a hard disc or the like.

The users who wish to use the data request for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

The database 2 which has received the request for use of the data M encrypts the data M by the crypt key Kd which is a permit key Kp

$$Cmkd=E(Kd, M),$$

and transmits the encrypted data Cmkd to the data communication apparatus 5 of users via the communication line 7 and charges with the charging center 3.

The data communication apparatus 5 supplies the received encrypted data Cmkd to the user terminal 8 while the user terminal 8 decrypts the encrypted data Cmkd by the crypt key Kd which is stored in the recording medium

$$M=D(Kd, Cmkd).$$

(b) In the case where the crypt key is encrypted and the common crypt key is preliminarily distributed to users:

In this crypt key system, when users register to use the database, the common crypt key K0 is supplied to users with the recording medium such as ROM or flexible disc and the supplied common crypt key K0 is stored in the user terminal 8.

The database 2 encrypts the crypt key Kd by using the common crypt key K0

$$Ckdk0=E(K0, Kd),$$

and supplies encrypted crypt key Ckdk0 to the broadcasting station 1.

The broadcasting station 1 broadcasts the received encrypted crypt key Ckdk0 supplied from database 2 by using the radio wave 6.

The receiving apparatus 4 supplies the received encrypted crypt key Ckdk0 to the user terminal 8 which decrypts the encrypted crypt key Ckdk0 in the beginning by the preliminarily stored common crypt key K0

$$Kd=D(K0, Ckdk0),$$

and stores the decrypted crypt key Kd in the recording medium such as a semiconductor memory, a flexible disc or a hard disc.

Users who wish to use the data requests for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

The database 2 which receives the request for the data usage encrypts the data M which is demanded for usage encrypts data M by the crypt key Kd

$$Cmkd=E(Kd, M),$$

and transmits it to the data communication apparatus 5 via the communication line 7 and chargess with the charging center 3.

The data communication apparatus 5 supplies the received encrypted data Cmkd to the user terminal 8 which decrypts the encrypted data Cmkd by the stored crypt key Kd

$$M=D(Kd, Cmkd).$$

(c) In the case where the crypt key is encrypted and the common crypt key is distributed to the user together with the encrypted data:

In this crypt key system, the database 2 encrypt the crypt key Kd by the common crypt key K0

$$Ckdk0=E(K0, Kd)$$

and supplies it to the broadcasting station 1.

The broadcasting station 1 broadcasts the encrypted crypt key Ckdk0 which has been supplied from the database 2, by using the radio wave 6.

The receiving apparatus 4 supplies the received encrypted crypt key Ckdk0 to the user terminal 8. The user terminal 8 stores the encrypted crypt key Ckdk0 in recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

Users who wish to use the data request for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

The database 2 which receives the request for the data usage encrypts the data M which is demanded for use by the crypt key Kd

$$Cmkd=E(Kd, M),$$

and transmits it to the data communication apparatus 5 via the communication line 7 together with the common crypt key K0 and charges with the charging center 3.

The data communication apparatus 5 supplies the received encrypted data Cmkd and the common crypt key K0 to the user terminal 8. The user terminal 8 decrypts the encrypted crypt key Ckdk0 which has been stored in the recording medium by the common crypt key K0

$$Kd=D(K0, Ckdk0),$$

and decrypts the encrypted data Cmkd by the decrypted crypt key Kd

$$M=D(Kd, Cmkd).$$

Summary of the Invention

The present invention provides a concrete structure for applying the invention of the crypt key system described in the previous applications to the television system, the database system or the electronic commercial transaction system or the like.

This system comprises a broadcasting station, a database, a receiving apparatus, a data communication apparatus, and a user terminal. As the crypt key system, secret-key cryptosystem and the public-key cryptosystem are used. In addition, the digital signature is used, and the crypt key is supplied through broadcasting with either encrypted or uncrypted.

The present invention is effective in the prevention from unjustified use or the copyright management in the database system, a pay-per-view system, or a video-on-demand system. Furthermore, the present invention is a useful means in the realization of an electronic market using the electronic data interchange system.

Brief Description of the Drawings

Fig. 1 is a structural view of a crypt key system according to the prior applications.

Fig. 2 is a structural view of the crypt key system according to a first embodiment of the present invention.

Fig. 3 is a structural view of the crypt key system according to a second embodiment of the present invention.

Fig. 4 is a structural view of the crypt key system according to third and fourth embodiments of the present invention.

Figs. 5(a), 5(b) and 5(c) are structural views of fifth embodiment to which the present invention is applied.

Embodiments

Embodiments of the present invention will be described by using Figs. 2 through 4.

[Embodiment 1]

A system shown in Fig. 2 is a crypt key system of the embodiment 1 in which the present invention is applied to a database system. This system comprises a broadcasting station 11 which either a multiplex broadcasting by of BS, CS, a terrestrial wave television, or FM broadcasting or the like, or data broadcasting by a digital broadcasting, a database 12 in which various kinds of data including moving picture data is stored, a charging center 13, a receiving apparatus 14 for receiving the data broadcasting offered by the broadcasting station 11, a data communication apparatus 15 for communicating with the database 12 and the user terminal 18 for using the data.

The database 12 and the broadcasting station 11, and the database 12 and the charging center 13 are connected with a direct means connecting with a communication line such as a dedicated line or an indirect means such as a flexible disc or the like. The database 12 and the data communication apparatus 5 are connected with a communication line 17 such as a communication line, or CATV line or the like. Then, the broadcasting station 11 and the receiving apparatus 14 are connected with a radio wave 16 such as a terrestrial wave television broadcasting, satellite television broadcasting, CATV broadcasting, FM broadcasting or a satellite data broadcasting or the like. The receiving apparatus 14 and the user terminal 18, and the data communication apparatus 15 and the user terminal 18 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc or the like.

What is shown with a solid line in Fig. 2 is an uncrypted data path and what is shown with a broken line is an encrypted data path.

Incidentally, data exchange between the database 12 and the broadcasting station 11, and the database 12 and the charging center 13 are, in principle, carried out with a dedicated line or a flexible disc. In addition, a public line, a broadcasting satellite, a communication satellite or a terrestrial wave broadcasting can be used. In such a case, the data is encrypted.

In this system, the secret-key cryptosystem and the public-key cryptosystem are used.

The database 12 prepares the public-key Kbd and the private-key Kvd to supply the public-key Kbd to the broadcasting station 11. The broadcasting station 11 which receives the public-key Kbd broadcasts it by a teletext multiplexing broadcasting using scanning lines during the retrace blanking interval period of an arnalog television picture signal, the data broadcasting using a sub audio band of the analog television audio signal, FM multiplex data broadcasting or digital data broadcasting.

Further, in this case, a digital signature of the database 11 can be done to the public-key Kbd.

The data may be supplied without encrypting the menu in which the titles of data which can be used, the content introduction of the data, product catalogs, order forms, blank checks, the copyright information for the convenience of the data usage.

The receiving apparatus 14 which receives the transferred public-key Kbd sends the public-key Kbd to the user terminal 18. The user terminal 18 which receives the transferred public-key Kbd stores the public key Kbd in the recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

Users who select the data which they request for usage by means of menu or the introduction of contents request for the use of data M to the database 12 via a communication line 17 by the data communication apparatus 15.

At this time, the user encrypts the public-key Kbd of the database 12 by own secret-key Ksu which has received from the database 12

$$Cksukbd=E(Kbd, Mksu)$$

and transmits it to the database 12

The database 12 decrypts the encrypted secret-key Cksukbd of the user by the private-key Kvd

$$Ksu=D(Kvd, Cksukbd)$$

and encrypts the data M which is requested for use by the decrypted user secret-key Ksu

$$Cmksu=E(Ksu, M),$$

and transmits it to the data communication apparatus 15 of the user via the communication line 17.

The user who receives the data Cmksu encrypted by own secret-key Ksu decrypts the encrypted data Cmksu with the user terminal 18

$$M=D(Ksu, Cmksu)$$

to use it.

This system is provided with charging center 13 which is incorporated with the database 12. This charging center 13 is used when the data is provided with pay basis. In the case where the data is one which is provided with free such as shopping information or the like, this charging center 13 is not used. However, even the data provided with free such as shopping information or the like, the charging center is used in the case where charges are to be settled along with orders.

[Embodiment 2]

Fig. 3 shows a crypt key system according to embodiment 2 in which the present invention is applied to a video on demand (VOD) system which broadcasts television programs corresponding to the requests from users.

This system comprises a CATV station 21, a charging center 23, a receiving apparatus 24, a data communication apparatus 25 and a user terminal 28.

The charging center 23 is used when the television program is provided on pay basis but not used when the television program is provided without charges along with advertisement.

In this system, the encrypted television broadcast programs and the crypt key are transmitted with the CATV line 27 which is a single path.

The CATV station 21 and the charging center 23 are connected with a direct means for electrical connection with a communication line such as a dedicated line or the like, or an indirect means such as flexible disc or the like. The CATV station 21 and the receiving apparatus 24, the CATV station 21 and the data communication apparatus 25 are connected with the CATV cable 27. The receiving apparatus 24 and the user terminal 28, the data communication apparatus 25 and the user terminal 28 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc or the like.

What is shown with a solid line in Fig. 3 is an uncrypted data path and what is shown with a broken line is an encrypted data path.

Incidentally, the data exchange between the CATV station 21 and the charging center 23 is carried out through a dedicated line or a flexible disc in principle. Additionally, the data exchange is also carried out by means of the communication line or the broadcasting satellite, the communication satellite and the terrestrial wave broadcasting. In this case, the data is encrypted.

In this system, the CATV system is treated as one kind of database. As a crypt key method, the secret-key cryptosystem and the public- key cryptosystem are adopted.

Users who use this VOD system either registers their own public-key Kbu with the CATV station 21 in advance, or transmit the public-key Kbu by using the communication apparatus 25 at the time when the request for usage.

The CATV station 21 encrypts the secret- key Ksb of the CATV station 21 by the transmitted public- key Kbu of users

$$Cksbkbu=E(Kbu, Ksb)$$

and transmits it to the data communication apparatus 25 via the CATV line 27

The television program M is encrypted by using the secret-key Ksb of the CATV station 21

$$Cmksb=E(Ksb, M)$$

and is broadcast to the receiving apparatus 24 via the CATV line 27.

The user decrypts the received encrypted secret-key Cksbkbu of the CATV station 21 by the private-key Kvu of user

$$Ksb=D(Kvu, Cksbkbu)$$

and decrypts the encrypted television program Cmksb using the decrypted secret-key Ksb of the decrypted CATV station 21

$$M=D(Ksb, Cmksb)$$

for use.

In addition, this crypt key system is applicable, if encryption is available, to the television broadcasting other than CATV, audio broadcasting, or data broadcasting. As a method for transmitting the crypt key from the broadcasting station, the teletext multiplex broadcasting using the scanning lines during the retrace blanking inverval of an analog television ppicture signal, the data broadcasting using an sub audio band of the analog television audio signal, FM multiplex data broadcasting, or digital data broadcasting can be also used.

In addition, this crypt key system can be used when the crypt key is distributed in the data copyright management system which is described in prior Japanese Patent Applications Nos. 6-64889, 6-237673, 6-264199, 6-264201 and 6-269959 proposed by the present inventor.

This crypt key system can be also applied to a case where a recording medium such as a CD-ROM or the like in which a plurality of informations are encypted with a plurality of different patterns and are recorded, which is described in Japanese Laid-Open Patent Application No. 6-132916, proposed by the present inventor.

These inventions of previous applications are explained hereinbelow.

An outline of the data copyright management system described in Japanese Patent Application No. 6-64889 is described as follows.

To control the copyright in the display (including the process to sound), storage, copy, edit and transfer of digital data in the database system including a real time transmission of a digital picture, any one or a plurality among a program for managing the copyrights a copyright information and a copyright management message are transmitted, when needed, in addition to a permit key for allowing the use of encrypted data corresponding to usage requests from users.

The copyright management message is displayed on a screen and advises or warns to the user in case the data is utilized other than the conditions of user's request or the permission. T the copyright management program watches and controls in order that the data is not utilized beyond the conditions of user's request or the permission.

The copyright management program, the copyright information and the copyright management message are supplied together with a permit key in some cases, or they are supplied together with data in some other cases. Or, a part of them is supplied together with the permit key, and other part is supplied with the data.

For data, the permit key, the copyright management message, the copyright information and the copyright management program, there are the following three cases: a case where these are transmitted with encrypted, and upon using, the encryption is decrypted, a case where they are transmitted with encrypted and remain in encrypted except being decrypted only when they are displayed, and a case where they are not encypted at all.

An outline of the data copyright management system described in Japanese Patent Application No. 6-237673 is described as follows.

This database copyright management system comprises a database in which uncrypted data is stored, a data supply means of a broadcasting station such as satellite broadcasting station for broadcasting the encrypted data from the database, or of a recording medium such as a CD-ROM where encrypted data from the database is recorded, a communication network, a key control center for controlling a crypt key, and a copyright management center for controlling copyrights of the database. Then, the database utilization program for using the database, the copyright management program for controlling the copyrights, a first crypt key and a second crypt key are used.

A first user registers with the key control center in advance for using the database. At that time, the database use program is distributed. This database utilization program includes information on the first user and a program for generating a crypt key unique to the first user with a predetermined algorithm by using the information.

The data is stored in the database without encrypted, and when it is distributed by broadcast, or through recorded on a recording medium or a communication network, the data is encrypted by the first crypt key to an encrypted data.

The encrypted data is stored in recording medium such as a semiconductor memory of the first user terminal, a flexible disc or hard disc, when distributed via broadcasting or communication network, is stayed as is when recorded in a CD-ROM recording medium and distributed, or is stored in the recording medium such as a semiconductor memory of the first user terminal, a flexible disc or a hard disc or the like.

The first user who uses the data directly from the database requests a key for decrypting and using the encrypted data to the key control center via the communication network. Information concerning the first user is presented at this time.

The key control center transfers the information on the first user to the copyright management center while the copyright management center uses information I concerning the first user to generate a crypt key peculiar to the first user by a predetermined algorithm, and the generated first user crypt key is used to encrypt the copyright management program, the first crypt key and the

second crypt key to be transferred to the key control center.

The copyright management program encrypted by using the crypt key generated by using the information on the first user is peculiar to the first user.

The key control center which receives the encrypted copyright management program transmits to the first user terminal each of the encrypted copyright management program, the first crypt key and the second crypt key via the communication network. Then, the first user stores the received encrypted copyright management program, the first crypt key and second crypt key in a recording medium such as a semiconductor memory, a flexible disc, or a hard disc.

The first user generates the crypt key peculiar to the first user by using a database utilization program which is distributed in advance and using information on the first user with a predetermined algorithm. Then, the first user decrypts the encrypted copyright management program, the encrypted first and second crypt keys, and the encrypted data is decrypted by the decrypted first crypt key.

In the case of storing, copying and transferring the decrypted data, it is encrypted by the second crypt key decrypted with the decrypted copyright management program. Then, the encrypted data is stored in the recording medium such as the semiconductor memory of the first user terminal, the flexible disc or the hard disc or the like. When the first user uses the stored encrypted data, it is decrypted by using the second crypt key. Then, this operation is repeated for primary sue of the data.

When the encrypted data is copied on the external memory medium or is transferred to the second user terminal via the communication network, the first crypt key and the second crypt key are disued by the copyright management program. The first user then,cannot use the encrypted data.

At this time, when the encrypted data is stored in the first user terminal, uncrypted information on the first user is added to the encrypted data which is stored.

In the case where the first user uses the encrypted data gain, the first user obtains the first crypt key and the second crypt key from the copyright management center. With the regrant of the first crypt key and the second crypt key, it is confirmed that the second user exists which has received the copy or the transfer of the encrypted data from the first user, and the fact of the second user is recorded on the copyright management center.

The second user who has received the copied or transferred encrypted data requests for the secondary use of the encrypted data to the copyright management center. The second user is not required to register with the key control center preliminary, unlike the first user. At the time of the request for data use, with the presentation of the information of the first user from which the encrypted data has been copied or transferred to the copyright control center, the request is accepted. If the first user information is not presented at this time, the user is recognized to be the first user and not the second user who has received the copy or the transfer of the encrypted data from the first user. Thus, the request for the secondary use is not accepted.

The copyright management center which acepts the request of the secondary use transmits the second crypt key for decrypting the encrypted data, the third crypt key for reencrypting and redecrypting the decrypted data and the copyright management program for the aforementioned decryption, the reencryption and redecryption, to the second user.

The outline of the copyright management system described in the Japanese Patent Application Nc. 6-264199 is described as follows.

This copyright management system uses the first public-key prepared by the user,
the first private-key corresponding to the first public-key,
the second public-key, the second private-key corresponding to the second public-key, and the first secret-key and the second secret-key prepared by the database.

The database side encrypts the data which is not encrypted by using the first secret-key, and encrypts the first secret-key by the first public-key, and the second secret-key by the second public-key. These encrypted data and the encrypted first secret-key and second secret-key are transmitted to users.

The user decrypts the encrypted first secret-key by using the first private-key and decrypts the encrypted data by the decrypted first secret-key for use. Then, the user decrypts the encrypted second secret-key by the second private-key so that the decrypted second secret-key is used as a crypt key for data storage, copy and transfer after the decryption of the data.

The outline of the data copyright management system described in the Japanese Patent Application No. 6-264201 is described as follows.

In the case where new data is prroduced by editing a plurality of encrypted data which are obtained from the database and is encrypted to be supplied to others, the crypt key for a plurality of data which are original materials and edit program as editing process with a digital signature are used as a use permit key.

When the user who has received the edited and encrypted data requests for use by presenting the digital signature to the copyright management center, the copyright management center recognizes the editor on the basis of the digital signature. Only in the case where it is recognized that the editor is the authorized user of the edited data, the crypt key for use is provided to those who request for use.

The outline of a method described in the Japanese Patent Application No. 6-269959 is explained as follows.

A first user receives the encrypted data in which the original data is encrypted by the first crypt key from the database and decrypts the data at the time of usage. After that, the data is encrypted by a second crypt key generated with a predetermined algorithm using one out of the first crypt key, the first user data, and the data

usage frequency or a combination thereof, and is stored, copied and transferred.

When the second user requests the secondary use of the data, the data copyright management center generates the second crypt key with a predetermined algorithm by using one out of the first crypt key of the original data, the first user data and the data use frequency or a combination thereof to be provided to the second user.

The second user to whom the second crypt key is provided decrypts the encrypted original data by using the second crypt key for usage.

[Embodiment 3]

The system shown in Fig. 4 is a crypt key system of embodiment 3 where the present invention is applied to the database system or the VOD system.

Like the crypt key system shown in Fig. 3 of embodiment 2, in this crypt key system, the television broadcasting programs and the crypt key pass through a single path which is the CATV line; however, these may pass through different path, as a matter of couse.

This system comprises a CATV station 31 for data broadcasting, a data managing center 33 such as database, a video system or the like, a receiving apparatus 34, a data communication apparatus 35 and a user terminal 38.

The data managing center 33 and the CATV station 31 are connected with a direct means for connecting with a communication line such as a dedicated line or the like or with an indirect means such as flexible disc or the like. The CATV station 31 and the receiving apparatus 34, and the CATV station 31 and the data communication apparatus 35 are connected with the CATV line 37. Incidentally, instead of the CATV line 37, a communication line which is an appropriate data broadcasting or available for data communication can be used. The receiving apparatus 34 and the user terminal 38, and the data communication apparatus 35and the user terminal means are connected with a direct means such as a connection cable or with an indirect means such as a flexible disc.

What is shown with a solid line is an uncrypted data path in Fig. 4 and what is shown with a broken line is an encrypted data path.

The data is exchanged between the data managing center 33 and the CATV station 31 in principle with a dedicated line or a flexible disc. In addition, the data may be also exchanged with a communication line, a broadcasting satellite, a communication satellite and a terrestrial wave broadcasting. In such a case, the data is encrypted.

This crypt key system adopts the secret-key cryptosystem and a public-key cryptosystem.

The data managing center 33 prepares and supplies to the CATV broadcasting station 31 the public-key Kbd and the private-key Kvd common in all the data to be supplied and the secret-key Ksdi which is different from one data to another. The CATV station 31 encrypts the received secret-key Ksdi by using the public-key Kbd of the data managing center 33

$$Cksdikbd=E(Kbd, Ksdi)$$

and broadcasts it by multiplex teletext broadcasting using scanning lines during the retrace line blanking interval of the analog television picture signal, the data broadcasting using a sub audio band of the analog television audio signal, FM mutiplex broadcasting, or digital data broadcasting.

For convenience of the data usage, menu showing titles of available data and introduction of data outline can be also supplied without encrypted to promote the use.

User who selected the desired data requests by the menu or the content introduction requessts for using the data to the data managing center 33 via the CATV line 37 by using the data communication line 35 through the CATV station 31. At this time, the user transmits own public-key Kbu to the data managing center 33.

The data managing center 33 which has received the request for use from the user enctyps the data M by the secret-key Ksdi:

$$Cmksdi=E(Ksdi, M)$$

and transmits it to the user terminal 38. At that time, the private-key Kvd of the data managing center is encrypted by the public-key Kvu of the user who has requested the use Ckvdkbu=E(Kbu, Kbd) to be transmitted to the user terminal 38.

The user who receives the encrypted private-key Ckvdkbu of the data managing center decrypts the encrypted private-key Ckvdkbu by the user private-key Kvu

$$Kvd=D(Kvu, Ckvdkbu)$$

and decrypts the encrypted secret-key Cksdikbd by the decrypted private-key Kvd of the data managing center

$$Ksdi=D(Kvd, Cksdikbd)$$

decrypts the encrypted data Cmksdi by the decrypted secret-key Ksdi of the data managing center

$$M=D(Ksdi, Cmksdi)$$

and use it.

[Embodiment 4]

Since the system structure of embodiment 4 is the same as embodiment 3 shown in Fig. 4, explanation thereof will be omitted.

This system adopts the secret-key cryptosystem and the public-key cryptosystem as the crypt key systemsimilarly to embodiment. In embodiment 3, the private-key Kvd of the data managing center is encrypted

by the public-key Kbu of users who request for use while in embodiment 4, the private-key Kvd of the data managing center is distributed in advance by using the IC card or the like and stored in the user terminal. In embodiment 3 data M is distributed corresponding to the request for data usage, while in embodiment 4 the data M is broadcast by means of the CATV line or the satellite broadcasting irrespective of the request for data usage.

When the user subscribes a comprehensive contract for using the database with the data managing center, the private-key Kvd of the data managing center which is commonly used with all data to be supplied is previously distributed to users by a recording medium such as an IC card or the like or a CATV line 37, and stored in the semiconductor memory of the user terminal 38, the hard disc or a flexible disc .

The data managing center 33 prepares a secret-key Ksdi different for each supplying data and a public-key Kbd, and supplies them to the CATV station 31. The CATV station 31 which receives the secret-key Ksdi encrypts the secret-key Ksdi by the public-key kbd

$$Cksdikbd=E(Kbd, Ksdi)$$

and broadcasts it by means of teletext multiplex broadcasting using scanning lines during the retrace blanking interval of the analog television picture signal, data broadcasting using the sub audio band of the analog television audio signal, FM multiplex data broadcasting or digital data broadcasting.

At this time, for the convenience of the data usage, menu showing the titles of data which can be used, or a content introduction for explaining the data outline for promoting the data usage can be also supplied without encrypted.

The CATV station 31 encrypts the data Mby the secret-key Ksdi

$$Cmksdi=E(Ksdi, M)$$

and broadcasts it via the CATV line irrespective of the request for use.

The user incorporates desired data out of the data which is broadcast via the CATV line on the basis of the menu or the content introduction into the user terminal by using a receiving apparatus 34.

The user decrypts the encrypted secret-key Cksdikbd by the private-key Kvd of the data managing center which is stored in the semiconductor memory in the user terminal 38,a hard disc or a flexible disc

$$Ksdi = D(Kvd, Cksdikbd)$$

and decrypts the encrypted data Cmksdi by the decrypted secret-key Ksdi

$$M=D(Ksdi, Ksdikbd)$$

for use.

Other modifications of the embodiments for distributing the crypt key will be explained.

[Embodiment 5]

In aforementioned embodiments, the public-key Kbd of the data managing center is broadcast from the broadcasting station instead of the communication line. Thus, it is impossible to confirm whether the public-key Kbd is justified or not.

In such a case, the private-key Kvd of the data managing center is used for digital signature to the public-key kbd of the data managing center.

$$Skbdkvd=E(Kvd, Kbd)$$

to be broadcast together with the public-key Kbd of the data managing center.

The user recognizes the digital signature Skbdkvd by the received public-key Kbd of the data managing center

$$Kbd=D(Kbd, Skbdkvd)$$

and when it is justified, use the public-key.

[Embodiment 6]

In embodiment 5, in the case where the data managing center adopts the membership system for preliminarily registering the use of the database, the public-key Kbui of users who are members is also preliminarily registered with the data managing center.

The data managing center encrypts the public-key Kbd of the data managing center by the public-key Kbui of each user

$$Ckbdkbui=E(Kbui, Kbd).$$

Digital signature is made to the the public-key Kbd of the data managing center by using the private-key Kvd of the data managing center

$$Skbdkvd=E(Kvd, Kbd).$$

Then, the encrypted public-key Ckbdkbui different from one user to another and the digital signature Skbdkvd are sent to the broadcasting station to broadcast the received encrypted public-key Ckbdkbui and the digital signature Skbdkvd.

At this time, the uncrypted user identification information of each user is broadcast by adding to the encrypted public-key Ckbdkbui if necessary.

Uthe uer who has received the broadcast encrypted public-key Ckbdkbui and the digital signature Skbdkvd decrypts the encrypted public-key Ckbdkb of the data managing center by the public-key Kvui

$$Kbd=D(Kvui, Ckbdkbui)$$

and stores the decrypted public-key Kbd of the data managing center in the user terminal.

The user recognizes the digital signature Skbdkvd by the received public-key Kbd of the data managing center

$$Kbd=D\ (Kbd,\ Skbdkvd),$$

and if it is justified, uses the stored public-key Kbd of the data managing center.

In this manner, a crypt key different from one user to another can be distributed.

[Embodiment 7]

Users present their own public-key Kbu to the data managing center at each time of access or request to the data managing center.

The data managing center which receives the request from the user encrypts the requested data M by the public-key Kbu of the user

$$Cmkbu=E\ (Kbu,\ M)$$

and sends it to the broadcasting station. The broadcasting station broadcasts the received encrypted data Cmkbu.

The users who receives the broadcast encrypted data Cmkbu decrypts by the private-key Kvu of the user

$$M=D\ (Kvu,\ Cmkbu),$$

and use it.

Figs. 5(a) through 5(c) show the modified esamples which use the crypt key system of the present invention.

Each esample shown the structure in the figure is applied the crypt key system, in electronic market transaction using the electronic data interchange system, to the credit settlement in retail shops shown in Fig. 5 (a); the settlement by means of an electronic check shown in Fig. 5 (b); and the whole sale conducted by makers and the like shown in Fig. 5 (c).

In these systems, a digital signature is used in addition to the secret-key cryptosystem. These systems comprise a user 42, and a retail shop 43, a financial organization 44 or a sholesaler 45 such as a maker the like which is a World Wide Web (WWW) server on the internet.

[Embodiment 8]

In the credit settlement in the shop shown in Fig. 5 (a), the shop 43 broadcasts a data Ms such as order form format, credit card format, advertisements, catalogs, preview, products description, and content introduction of a database, and menu, charge schedule and price list, via the satellite 41 and a CATV line.

User 42 who receives the data Ms such as order form format and a public-key Kbs of the shop 43 encrypts the user secret-key Ksu by the public-key Kbs of the shop 43

$$Cksukbs=E\ (Kbs,\ Ksu)$$

and enters Mu items such as the order content, the payment amount and a credit card number with encrypted by the secret-key Ksu of user 42 on the basis of information such as advertisement, catalog, products description and charges/prices list

$$Cmuksu=E\ (Ksu,\ Mu),$$

when needed, compresses Mu into a compressed document mu and sign by digital signature by the private-key Kvu of the user 42

$$Smukvu=E\ (Kvu,\ mu),$$

and transmits it to shop 43 attached with the public-key Kbu of the user 42 via the network 47.

The shop 43 which has received the order decrypts the encrypted secret-key Cksukbs of the user 42 by the private-key Kvs of the shop 43

$$Ksu=D\ (Kvs,\ Cksukbs),$$

and decrypts the encrypted order document Cmuksu by the decrypted secret-key Ksu of the user 42

$$Mu=D\ (Ksu,\ Cmuksu).$$

Then, order acceptance is executed.

When the digital signature Smukvu is recognized by the public-key Kbu which the user 42 attached

$$mu=D\ (Kbu,\ Smukvu),$$

a receipt is sent to the user 42 via the network 47.

In this system, it is possible to prevent the unjustified use of the credit number because the credit card number entered in the order form is sent with encrypted.

Further, the following process enables reliable transaction:

The shop 43 compresses the digital data Ms1 of the order form format, the credit card format, advertisement, catalog, a preview, products description, and content introductionof the database and menu/charge schedule/price list into a compressed document msl, with digital signature by the private-key Kvs of the shop 43

$$Smslkvs=E\ (Kvs,\ msl)$$

and broadcasts it attaching the public-key Kbs of the shop 43 so that users recognizes the digital signature Smslkvs by using the public-key kbs of the shop 43

$$ms'=D\ (Kbs,\ Smskvs).$$

[Embodiment 9]

In the settlement by means of electronic checks shown in Fig. 5 (b), the bank as financial organization 44 broadcasts the blank check format Mf which is digital data attached with the publlic-key Kbf of the bank 44 via the satellite 41 or the CATV line.

The user 42 who receives the blank check format Mf encrypts the secret-key Ksu of the user 42 by the bank public-key Kb

$$Cksukbf=E(Kbf, Ksu),$$

enters Mu items concerning a payee and the payment amount with encrypted by the secret-key Ksu of the user 42

$$Cmksu=E(Ksu, Mu),$$

when needed, compresses Mu to the compressed document mu, and sign by digital signature by using the private-key Kvu of the user 42

$$Smukvu=E(Kvu, mu)$$

and transmits them attaching the public-key Kbu of the user 42 and the encrypted secret-key Cksukbf of the user 42 which is encrypted by the the public-key Kbf of the bank 44 to the bank 44 via the network 47.

The bank 44 which receives the described check uses the bank private-key Kvf to decrypt the encrypted secret-key Cksukbf of the user 42

$$Ksu=D(Kvf, Cksukbf),$$

decrypts the encrypted data Cmuksu of the payee and the payment amoount by the decrypted user secret-key Ksu

$$Mu=D(Ksu, Cmuksu)$$

and recognizes the described content, and the currency exchange process is executed.

Furthermore, the bank recognizes the user 42 by Smuksu with the digital signature using the public-key Kbu added by the user 42

$$mu'=D(Kbu, Smuksu)$$

encrypts the confirmation document Ms2 by the public-key Kbu added by the user 42

$$Cms2kbu=E(Kbu, Ms2)$$

and send it back to the user 42 via a network 47.

The user who receives the encrypted confirmation document Cms2kbu from the bank 44 decrypts the encrypted confirmation document Cms2kbu by the private-key Kvu of the user 42

$$Ms2=D(Kvu, Cms2kbu)$$

and confirms the content.

According to the system, since the patty to which the payment is made and the payment amount are encrypted and described in the check, it is possible to prevent the unjustified use of the content described in the check.

In addition, the blank check format Mf which is digital data is xmpressed into a compressed document mf and signed by digital signature by using the private-key Kvf of the bank 44

$$Smfkvf=E(Kvf, mf)$$

to be broadcast attaching the public-key Kbf of the bank 44. The user recognizes the digital signature Smskvs by the public-key Kbs of the bank 44

$$mf'=D(Kbf, Smfkvf).$$

The confirmation document Ms is further compressed into a compressed document ms with digital signature by using the public-key Kbu added by the user

$$Smskbu=E(Kbu, ms)$$

Thus, the bank can recognize the user who has entered on the check.

[Embodiment 10]

At the sholesaler 45 of a maker or the like shown in Fig. 5 (C), the wholesaler 45 forms a proforma invoice format Mw1 into a compressed data mwl and sign by digital signature by using the private-key Kvw of the wholesaler 45

$$Smwlkvw=E(Kvw, mwl)$$

and broadcasts it attaching the public-key Kbw of the wholesaler 45 via the satellite 41 or CATV line.

The user 42 Which is a shop receives the broadcast proforma invoice format Mwl and the public-key Kbw of the wholesaler 45, and encrypts the proforma invoice request Mu by the public-key Kbw of the wholesaler 45

$$Cmukbw=E(Kbw, Mu)$$

and transmits it to the wholesaler 45 via the network 47.

At this time, the proforma invoice request Mu is compressed to compressed data mu when needed, and signed by the digital signature by using the private-key Kvu of the user 42

$$Smkvu=E(Kvu, mu)$$

to be transmitted together with the public-key Kbu of the user 42 to the wholesaler 45.

The wholesaler 45 which receives the encrypted proforma invoice request Cmukbw decrypts the encrypted proforma invoice request Cmukbwby the private-key Kvw of the wholesaler 45

Mu=D (Kvu, Cmukbw)

and recognizes the described proforma invoice request Mu.

Further, the whole saler 45 recognizes the digital signature Smkvu by the public-key Kbu of the user 42

mu=D (Kbu, Smkvu)

and estimates to the proforma invoice and encrypts the proforma invoice Mw2 by the public-key Kbu of the user 42

Cmw2kbu=D (Kbu, Mw2)

and then, transmit it to the user 42 via the network 47.

The user 42 who receives the encrypted proforma invoice Cmw2kbu from the wholesaler 45 decrypts it by the private-key Kvu of the user 42

Mw2=D (Kvu, Cmw2kbu).

According to this system, since the public-key and the private-key are used, there is no fear that the content of the proforma invoice is stolen to be used and also different proforma invoice can be made for each user.

In the systems shown in Figs. 5 (a) through 5 (c), since each format and advertisement with no need of secrecy are broadcast via satellite or CATV broadcasting, the data can be effectively transmitted.

As explained above, a multimedia system can be realized which combines general information media such as television broadcasting and audio broadcasting with data communication media using computers by using the crypt key system of the present invention, whhile the general information media and the data communication media has been existing so far as an independent system each.

A concrete structure for realizing the multimedia system will be explained as follows.

The current television broadcasting is provided by means of an analog system through terrestrial wave broadcasting, satellite broadcasting or CATV broadcasting. In the meantime, most general data communication line is a public telephone line.

In such a system structure, the crypt key system according to embodiment 1 shown in Fig. 2 can be used as a basic structure of a system for realizing a video-on-demand. The broadcasting station broadcasts the public-key Kbb in multiplexing with the sub audio band of an audio zone in the scanning line of the vertical retrace interval of an analog television broadcasting program.

Users who wish to use the television program encrypt their own secret-key Ksu by the public-key Kbb broadcast from the broadcasting station.

CKsukbb=E (Kbb, Ksu)

and request for the usage by transmitting the the encrypted secret-key Cksukbb to the broadcasting station via a communication line.

The broadcasting station decrypts the encrypted secret-key Cksukbb of the users by the private-key Kvb of the broadcasting station.

ksu=D (Kvb, Cksukbb)

scrambles the broadcasting program by the decrypted secret-key Ksu and broadcasting it.

The users descrambles the scrambled program for use by their own secret-key Ksu.

By adopting such a structure, persons other than users those who request to use the program cannot use the program.

As a basic structure of a system for realizing the video on demand and pay-per-view in such a system structure, the crypt key system shown in embodiment 4 or embodiment 5 in Fig. 4 can be used.

The broadcasting station 31 encrypts by the secret-key Ksb of the broadcasting station 31 the public-key Kbb of the broadcasting station 31

Cksbkbb=E (Kbb, Ksb)

and broadcasts it via the communication line 37 in multiplexing with the scanning line or a sub audio band of the retrace interval of the analog television broadcasting program.

User 38 who wishes to use the television program 38 requests for the usage by transmitting own public-key Kbu to the broadcasting station 31 via the communication line 37.

The broadcasting station 31 scrambles the broadcasting program by the secret-key Ksb of the broadcasting station and broadcasts it via the communication line 37. At this time, the private-key Kvb of the broadcasting station 31 is encrypted by the public-key Kbu of user 38

Ckvbkbu=E (Kbu, Kvb)

and is broadcast via the communication line 37.

The user 38 decrypts the encrypted private key Ckvbkbu of the broadcasting station 31 by own private-key Kvu

Kvb=D (Kvu, Ckvbkbu),

decrypts the encrypted secret-key Cksbkbb of the broadcasting station 31 by the private-key Kvb of the decrypted broadcasting station 31.

Ksb=D (Kvb, Cksbkbb)

and descrambles the scrambled broadcasting programby the decrypted secret-key Ksb of the broadcasting station 31.

By adopting such a structure, persons other than users who request to use the program cannot use them.

Further, the crypt key system can be applied to television shopping which is frequently conducted currently by combining the television broadcasting and the telephone.

In the currently conducted television shopping which uses the analog television broadcasting, product introduction and sales method are presented on the television screen so that users record information on the sales method manually and request for the purchase thereof by a telephone on the basis of the recorded information.

On the contrary, the crypt key system according to the present invention proposes a transmission of data of the order format and the check format in multiplexing with the scanning line of the vertical retrace interval or the sub audio band of the audio zone.

In the meantime, an apparatus called personal computer television set which integrates the personal computer and the television set or an apparatus which combines a video capture device which is realized as an IC card, a PC card or an insertion board and a personal computer allows incorporation of the television picture.

With the combination of the multiplex data such as an order format and a check format with a video capture device, an electronic television shopping can be conducted.

In such a television shopping, when the television shopping product introduction display is broadcast, the order format and the check format are broadcast in data multiplex with the scanning line of the vertical retrace interval or the sub audio band of the audio zone.

If the users operate the apparatus when the product introduction display of the desired product to purchase is broadcast, the order format and the check format data are incorporated with the static display picture.

Users who wish to use the television shopping enters necessary items on the order format or check format to request for the purchase. To secure the safety of the transaction at this time, encryption by the public-key cryptsosystem or the secret-key cryptosystem and digital signature are used with the system according to embodiments 1 to 5.

At this time, the content of transaction can be confirmed when the purchase order is requested by adding the static display picture of the product introduction together with the order and the check.

As a simple method, the order form format and the check format may be also transmitted as a television picture so that necessary items are entered on the order format and the check format which are incorporated as a static display picture.

In addition, the order form format and the check format can be transmitted via facsimile broadcasting which is multiplexed with the sub audio band of the audio zone.

By adopting such a method, an electronic market using electronic data intercahnge (EDI) by means of a current analog television method can be realized with the television shopping.

These video-on-demand system and the pay-per-view system can be applied to the digital television broadcasting other than the analog television broadcasting.

In the case where a CATV line is used as a communication line, both the broadcasting and data communication can be carried out with the CATV line only.

Further, these video-on-demand system and pay-per-view system can be also applicable to transmission of high-quality audio data and moving picture data performed in computer communication network system using low-speed public telephone line or high-speed integrated services digital network (ISDN) or in internet system connecting a plurality of computer communication network.

As an apparatus to be used, the receiving apparatus and the communication apparatus can be incorporated in the television set. Apparatuses can be also constituted as a separate apparatus by using a set top box or the like.

In addition, a constitution an apparatus referred to as a personal computer television set which is gradually prevalent or by combining a video capture device which is realized as an IC card a PC card or an insertion board for transmitting a television signal to the personal computer can be used.

Claims

1. Crypt key system comprising a broadcasting station (1), a database (2), a receiving apparatus (4), a data communication apparatus (5) and a user terminal (8), wherein
said database (2) and said broadcasting station (1) are connected with an online communication means such as a dedicated line, or the like or a off-line means such as a flexible disc or the like;
said database (2) and said data communication apparatus (5) are connected with a communication line (7) ;
said broadcasting station (1) and said receiving apparatus (4) are connected with a radio wave (6);
whereas between said receiving apparatus (4) and said user terminal (8) and between said data communication apparatus (5) and said user terminal (8) said are connected with direct online means or with off-line means such as a flexible disc;
said database (2) prepares a public-key and a private-key and supplies said public-key to said broadcasting station (1);
said broadcasting station (1) broadcasts said received public-key;
said receiving apparatus (4) transmits said received

public-key to said user terminal (8);
said user terminal (8) stores said transmitted public-key;
a user encrypts a secret-key of the user by said received public-key and transmits said secret-key at the time of request for the use of data which he desires, to said database (2);
said database (2) which has received the request for data use decrypts said secret-key of said user by said private-key and encrypts the data by said decrypted secret-key of said user to transmit the data to said data communication apparatus (5) via said communication line (7); and
said user transmits the received data to said user terminal (8) to decrypt said data by said secret-key.

2. Crypt key system according to claim 1 wherein a digital signature of said database (2) is provided on said public-key.

3. Crypt key system comprising a CATV station (31), a charging center, a receiving apparatus (34), a data communication apparatus (35), and a user terminal (38), wherein
between said CATV station (31) and said receiving apparatus (34) and between said CATV station (31) and said data communication apparatus (35) are connected with a CATV line (37);
between said receiving apparatus (34) and said user terminal (38) and between said data communication apparatus (35) and said user terminal (38) are connected with direct online means or with off-line means such as a flexible disc or the like;
a user preliminarily registers a public-key of said user with said CATV station (31) or presents said public-key of said user at the time of request for usage;
said CATV station (31) encrypts a secret-key which is a use permit key of said CATV (31) station by using said public-key of said user who has requested the usage and also encrypts a television program by said secret-key, to broadcast both via said CATV line (37); and
said user receives said encrypted television program and said secret-key with said receiving apparatus (34) and decrypts said secret-key by a private-key corresponding to said public-key for decrypting said television program by said decrypted secret-key.

4. Crypt key system comprising a CATV station (31), a data managing center (33), a receiving apparatus (34), a data communication apparatus (35) and a user terminal (38), wherein
said CATV station (31) and said data managing center (33) are connected with online communication means such as a dedicated line or the like, or off-line means such as a flexible disc or the like;
between said CATV station and said receiving apparatus (34) and between said CATV station and said data communication apparatus (35) are connected with a CATV line (37);
between said receiving apparatus (34) and said user terminal (38) and between said data communication apparatus (35) and said user terminal (38) are connected with direct online means or with off-line means such as a flexible disc or the like;
said data managing center (33) supplies a public-key, and a secret-key which is a use permit key for each data to be supplied, to said CATV station (31);
said CATV station (31) encrypts said secret-key for each data by said public-key of data managing center (33) to broadcast;
a user requests for the use of data by using said data communication apparatus (35) to said data managing center (EE) via said CATV line (37) together with transmitting a public-key of said user;
said data managing center (33) encrypts the data by said secret-key for each data, and encrypts said public-key of data managing center (33) by said public-key of said user and transmits encrypted data and encrypted said public-key of data managing center (33) together with a private-key of said data managing center (33) to said user;
said user decrypts said encrypted public-key of data managing center (33) by a private-key of said user, decrypts said encrypted secret-key for each data by decrypted said public-key of data managing center (33) and decrypts encrypted data by decrypted said secret-key for each data.

5. Crypt key system according to claim 4 wherein a digital signature of said data managing center (33) is provided on said public-key of data managing center (33).

6. Crypt key system comprising a CATV station (31), a data managing center (33), a receiving apparatus (34), a data communication apparatus (35), and a user terminal (38), wherein
a public-key of a user is registered with said data managing center (33) in advance;
said data managing center (33) encrypts a public-key of said data managing center (33) by said public-key of each user to provide a digital signature on said public-key of data managing center (33) by a private-key of said data managing center (33);
said encrypted public-key of said data managing center (33) and said digital signature of data managing center (33) are sent to said CATV station (31);
said CATV station (31) broadcasts said received encrypted public-key of data managing center (33) and said digital signature;
said user decrypts said received encrypted public-key of data managing center (33) by said public-key of said user and recognizes said digital signature by said decrypted public-key of data control center.

7. Crypt key system according to claim 6 wherein uncrypted user identification information of each user is further added to the encrypted public-key of said data managing center (33) to be broadcast.

8. Crypt key system comprising a CATV station (31), a data managing center (33), a receiving apparatus (4), a data communication apparatus (35), and a user terminal (38), wherein
a user presents a public-key of said user to said data managing center (33) upon requesting use of the data to said data managing center (33);
said data managing center (33) receives the request for data use from said user and encrypts the data requested by said public-key of said user to send to said CATV station (31) ;
said CATV station (31) broadcasts said received encrypted data; and
said user who receives said broadcast encrypted data decrypts said encrypted data by a private-key of said user.

FIG. 1

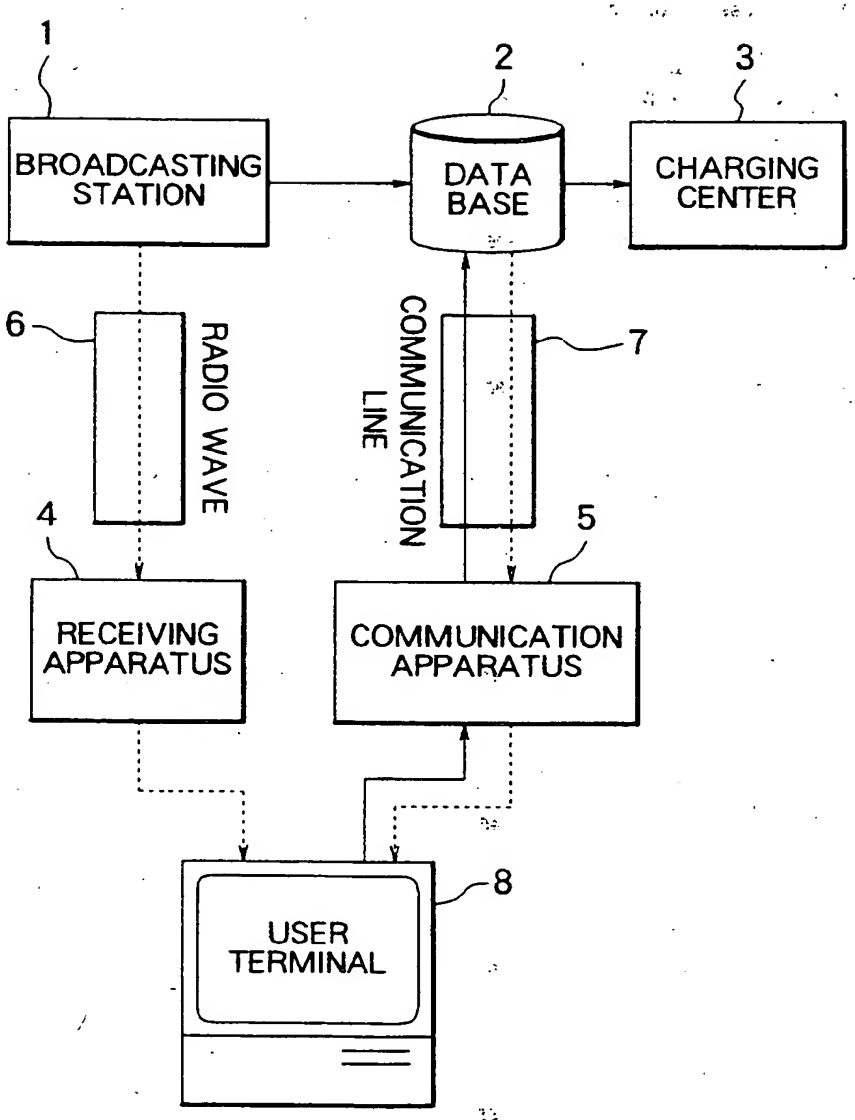


FIG. 2

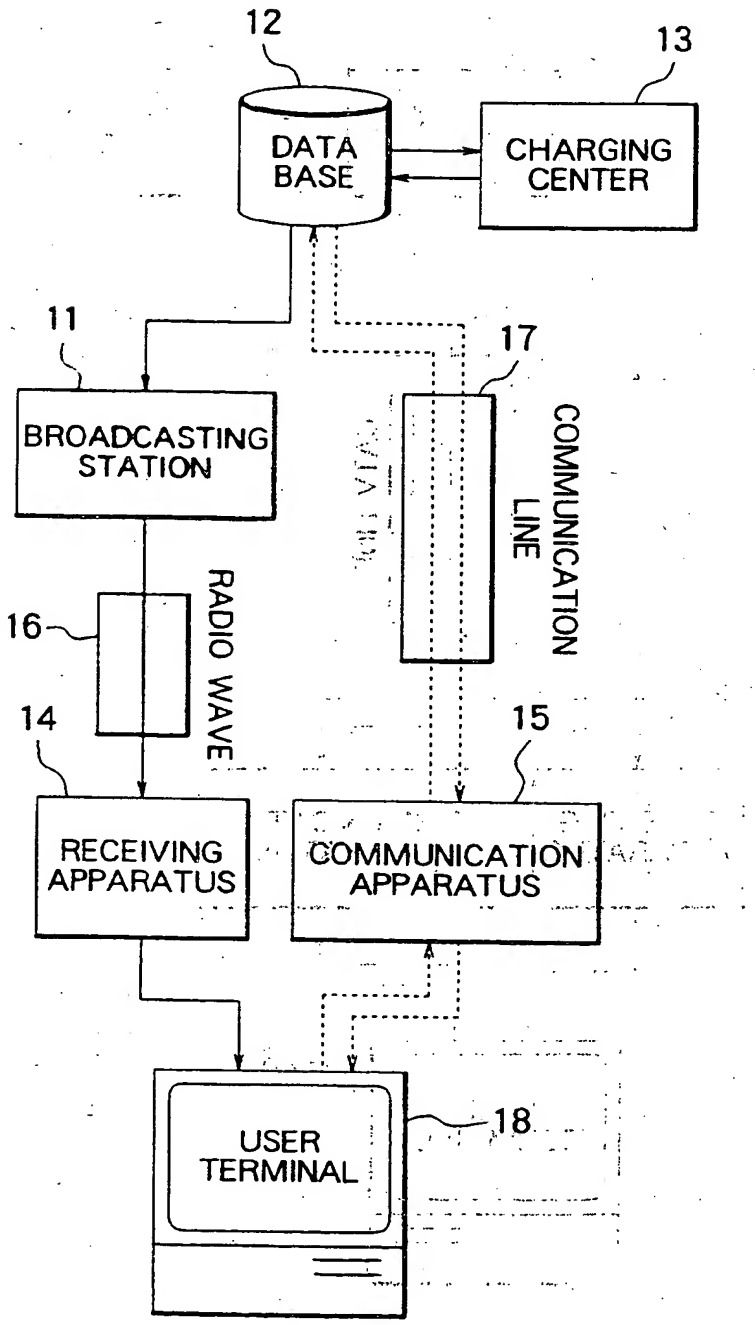


FIG. 3

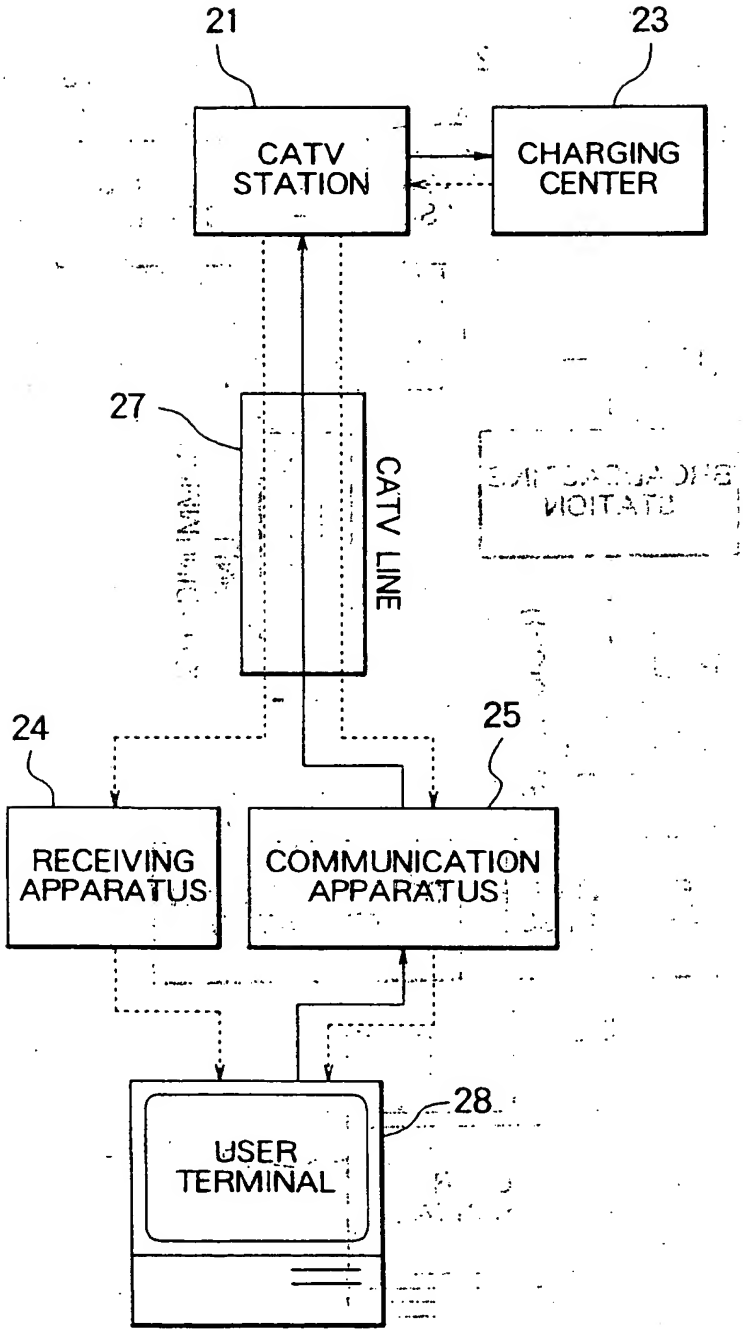


FIG. 4

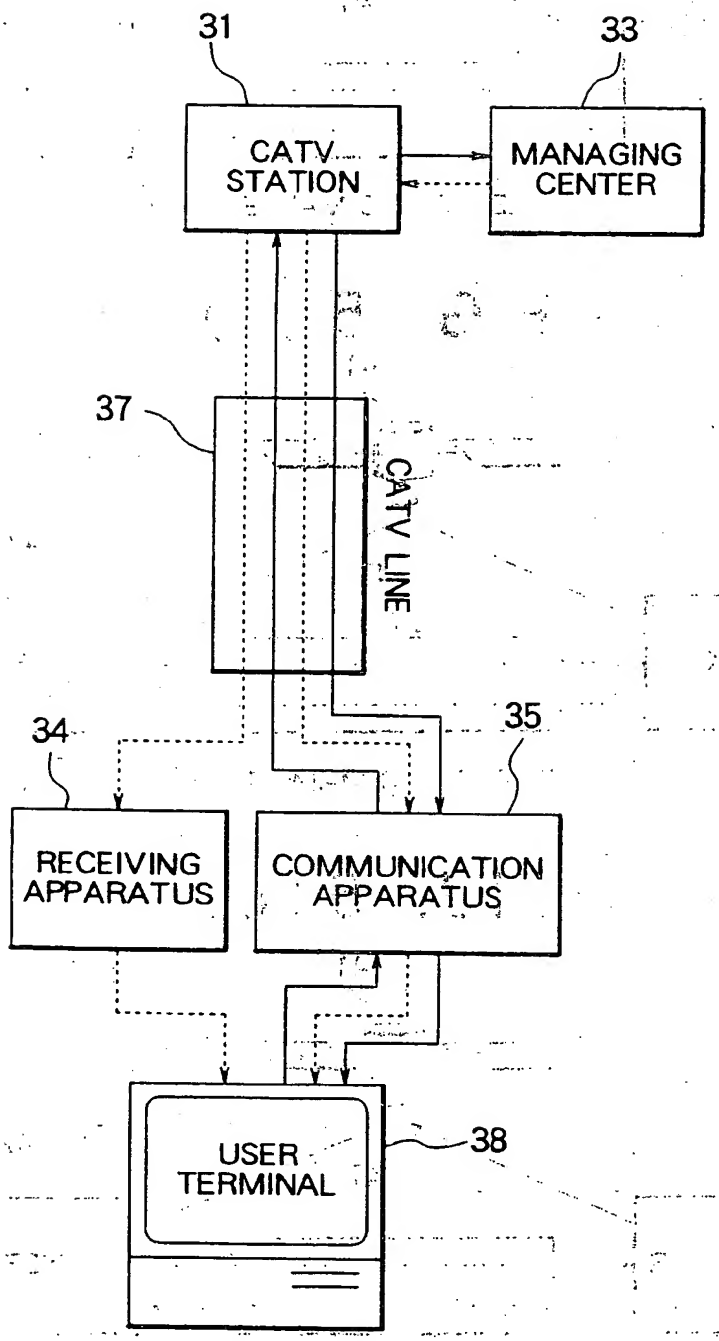


FIG. 5(a)

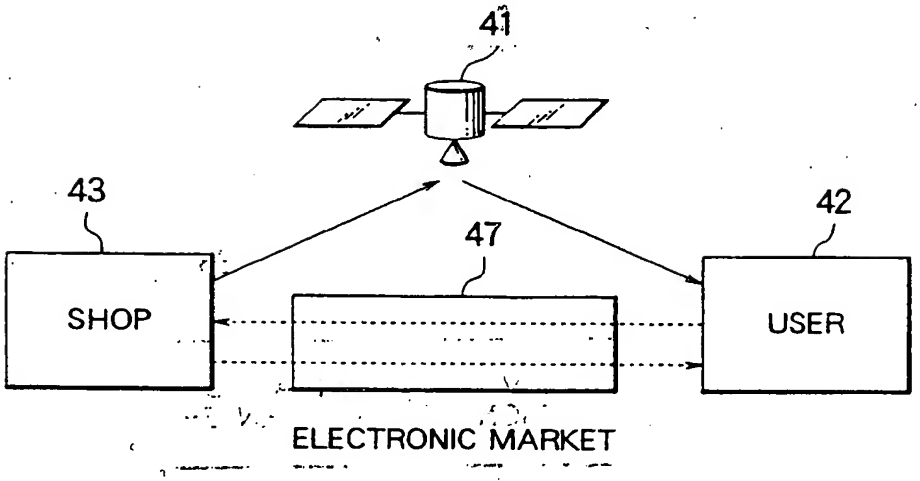


FIG. 5(b)

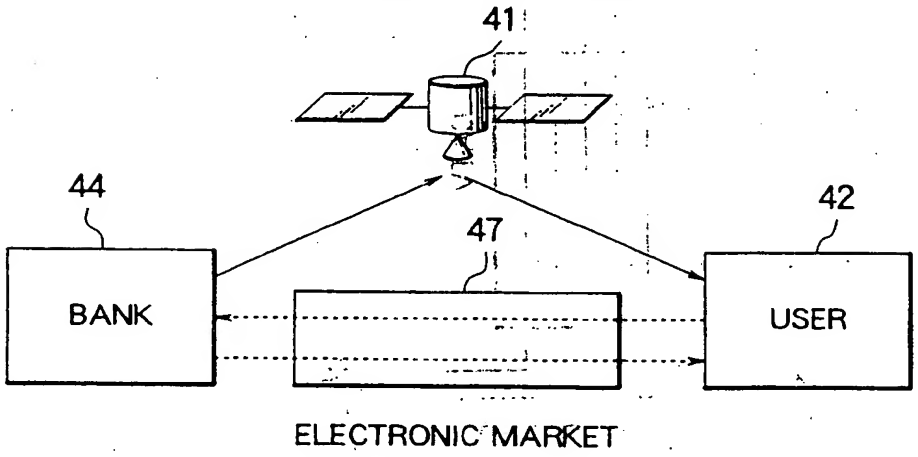
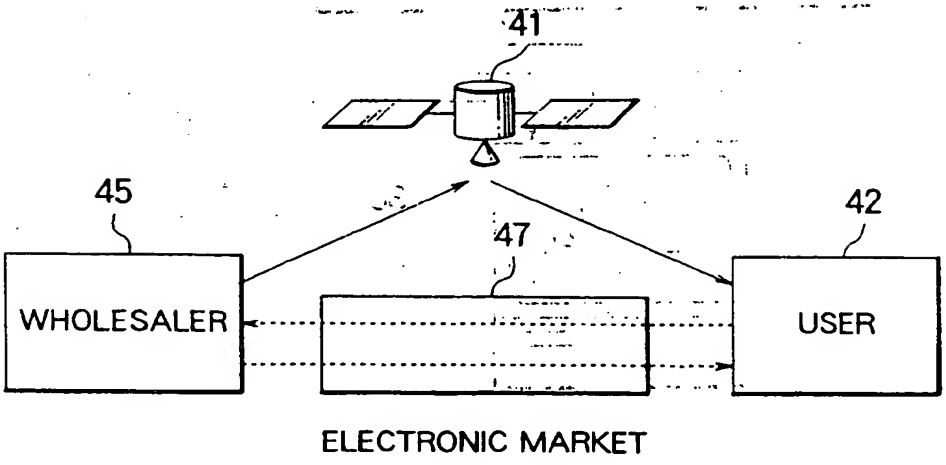


FIG. 5(c)



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 719 045 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
16.10.1996 Bulletin 1996/42

(43) Date of publication A2:
26.06.1996 Bulletin 1996/26

(21) Application number: **95119605.4**

(22) Date of filing: **13.12.1995**

(51) Int. Cl.[6]: **H04N 7/167**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **13.12.1994 JP 309292/94**

(71) Applicant: **MITSUBISHI CORPORATION**
Chiyoda-ku Tokyo 100 (JP)

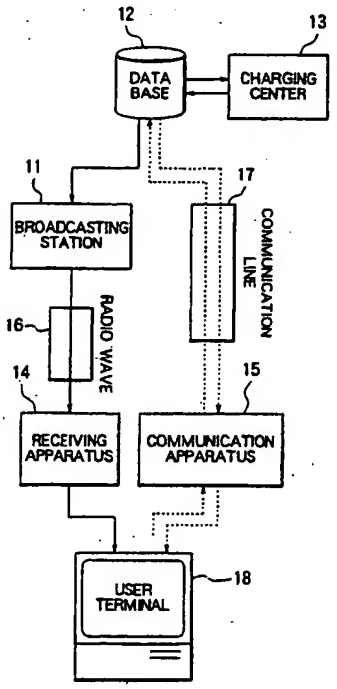
(72) Inventor: **Saito, Makato**
Tama-shi, Tokyo (JP)

(74) Representative: **Neidl-Stippler, Cornelia, Dr.**
Rauchstrasse 2
81679 München (DE)

(54) Crypt key system for broadcast programmes

(57) The invention relates to a crypt key system applicable to a television system, a database system or an electronic commercial transaction system or the like. This system consists of a broadcasting station 11, a database 12, a receiving apparatus 14, a data communication apparatus 15 and a user terminal 18. As a crypt key system, a secret-key cryptosystem, a public-key cryptosystem, and a digital signature system are used. The keys used in the system are either encrypted or remain uncrypted to be supplied by broadcasting. The present invention is effective in the prevention of an unjustified use of the database system, managing copyrights, and in a pay-per-view system and a video-on-demand system. Further, the present invention is effective in realizing an electronic market which uses an electronic data information system.

FIG. 2



A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 11 9605

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP-A-0 438 154 (CANON KK) 24 July 1991 * page 3, column 3, line 3 - line 31 * * page 4, column 5, line 49 - page 8, column 13, line 7 * * figures 1-5 *	1-8	H04N7/167
X	EP-A-0 506 435 (SCIENTIFIC ATLANTA) 30 September 1992 * page 1, line 5 - line 16 * * page 8, line 41 - page 13, line 2 * * page 14, line 55 - page 16, line 45 * * figures 7-10,12 *	1-8	
A	CABLE TV SESSIONS, MONTREUX, JUNE 10 - 15, 1993, no. SYMP. 18, 11 June 1993, POSTES;TELEPHONES ET TELEGRAPHES SUISSES, pages 761-769, XP000379391 VIGARIE J P: "A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL: THE TRANSCONTROLLER" * the whole document *	1-8	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04N
A	EP-A-0 450 841 (GTE LABORATORIES INC) 9 October 1991 * page 3, column 1, line 56 - page 5, column 6, line 58 * * figures 1.2 *	1-8	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	26 August 1996	Van der Zaal, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)